

#2
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

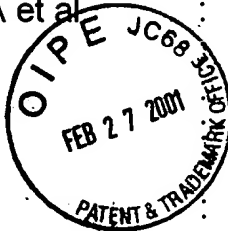
In re Application of:

Takayuki SUGAHARA et al

Serial No. 09/726,434

Filed: December 1, 2000

For: Method And Apparatus For
Contents Information



Art Unit: 2131

Examiner: not assigned

Atty Docket: 0102/0147

SUBMISSION OF PRIORITY DOCUMENTS

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Attached hereto please find a certified copy of applicants' Japanese application No. 2000-018437 filed in Japan on January 27, 2000.

Applicants request the benefit of said January 27, 2000 filing date for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

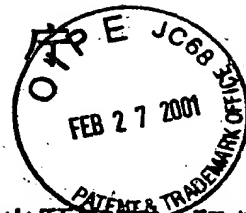
Louis Woo, Reg. No. 31,730
Law Offices of Louis Woo
1901 N. Fort Myer Drive, Suite 501
Arlington, Virginia 22209
Phone: (703) 522-8872

Date: Feb 27 2001

RECEIVED
MAR 01 2001
Technology Center 2100

U4-0025-TH

日 本 国 特 許
PATENT OFFICE
JAPANESE GOVERNMENT



RECEIVED
MAR 01 2001
Technology Center 2100

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 1月27日

出 願 番 号
Application Number:

特願2000-018437

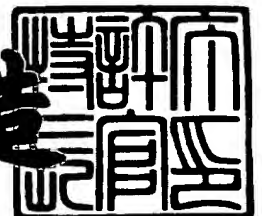
出 願 人
Applicant(s):

日本ビクター株式会社

2000年12月 8日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3101698

【書類名】 特許願

【整理番号】 411001711

【提出日】 平成12年 1月27日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 1/00
G09C 1/00

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 菅原 隆幸

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 黒岩 俊夫

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 猪羽 渉

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 上田 健二郎

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

【氏名】 日暮 誠司

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代表者】 守随 武雄
【電話番号】 045-450-2423
【手数料の表示】
【予納台帳番号】 003654
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ情報伝送方法、コンテンツ情報記録方法、コンテンツ情報伝送装置、コンテンツ情報記録装置、伝送媒体、及び記録媒体

【特許請求の範囲】

【請求項 1】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項 2】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

【請求項 3】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項 4】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の

鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

【請求項 5】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報を出力する第 1 の鍵情報暗号化手段と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第 1 の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送する伝送手段と、

を設けたことを特徴とするコンテンツ情報伝送装置。

【請求項 6】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報を出力する第 1 の鍵情報暗号化手段と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第 1 の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、

を設けたことを特徴とするコンテンツ情報記録装置。

【請求項 7】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とする伝送媒体。

【請求項 8】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とする記録媒体。

【請求項 9】

前記ID情報は、1 つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別IDに関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに関する情報、課金に関する情報のうちの 1 つ以上の情報であることを特徴とする請求項 3 記載のコンテンツ情報伝送方法、または請求項 4 記載のコンテンツ情報記録方法、または請求項 5 記載のコンテンツ情報伝送装置、または請求項 6 記載のコンテンツ情報記録装置、または請求項 7 記載の伝送媒体、または請求項 8 記載の記録媒体。

【請求項 1 0】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項 1 1】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情

報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

【請求項 1 2】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項 1 3】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

【請求項 1 4】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報を出力する第 1 の鍵情報暗号化手段と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と

前記暗号化第 1 の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送する伝送手段と、
を設けたことを特徴とするコンテンツ情報伝送装置。

【請求項 1 5】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得

た暗号化第 1 の鍵のもとになる情報を出力する第 1 の鍵情報暗号化手段と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と

、
前記暗号化第 1 の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、

を設けたことを特徴とするコンテンツ情報記録装置。

【請求項 1 6】

所定の縮退関数により特定の認証子値が得られるように設定された ID 情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記 ID 情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とする伝送媒体。

【請求項 1 7】

所定の縮退関数により特定の認証子値が得られるように設定された ID 情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記 ID 情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とする記録媒体。

【請求項 1 8】

前記 ID 情報は、1 つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別 ID に関する情報、複数人のグループを識別する識別 ID に関する情報、レーティングに関する情報、機器メーカーの識別 ID に関する情報、コンテンツプロバイダーの識別 ID に関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有 ID に関する情報、接続機器の固有 ID に関する情報、コンテンツの記録されたメディアの固有 ID に関する情報、コンテンツを識別する ID に関する情報、課金に関する情報のうちの 1 つ以上

の情報であることを特徴とする請求項 1 2 記載のコンテンツ情報伝送方法、または請求項 1 3 記載のコンテンツ情報記録方法、または請求項 1 4 記載のコンテンツ情報伝送装置、または請求項 1 5 記載のコンテンツ情報記録装置、または請求項 1 6 記載の伝送媒体、または請求項 1 7 記載の記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンテンツ鍵とそのコンテンツ鍵を用いて暗号化された暗号化コンテンツ情報を伝送、記録するためのコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体に関するものである。そして、この発明は、特にコンテンツ情報を正規の制限下においてのみの確に再生（復号）させることを可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供することを目的としている。

【0 0 0 2】

【従来技術】

暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのデジタルデータを配信する有用な方法として、特開平 1 0 - 2 6 9 2 8 9 のデジタルコンテンツ配布管理方法、デジタルコンテンツ再生方法及び装置がある。この発明では、デジタルコンテンツの配布側では、デジタルコンテンツを暗号化及び圧縮して加工し、この加工したデジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信する。そして、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、デジタルコンテンツの再生側では、その加工されたデジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。

【0 0 0 3】

また、特開平 1 0 - 2 8 3 2 6 8 の情報記録媒体、記録装置、情報伝送シス

テム、暗号解読装置では、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が追加記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーして不正使用をすることを防止しするようにしている。

【0004】

【発明が解決しようとする課題】

しかし、上記従来方式では、暗号化コンテンツ情報の再生（復号）に制限を加えて、正規の条件下以外の不正な再生（復号）を防止するようにしているが、その制限情報は第三者により容易に変更することが可能であり、不正な条件下での再生（復号）を的確に防止することが難しかった。

この発明は、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供することを目的としている。

【0005】

【課題を解決するための手段】

そこで、上記課題を解決するために本発明は、下記の各方法・装置を提供するものである。

（１） 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

（２） 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の

鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

(3) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第1の鍵のもとになる情報と、

前記第1の鍵のもとになる情報と前記特定の認証子値とから生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

(4) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第1の鍵のもとになる情報と、

前記第1の鍵のもとになる情報と前記特定の認証子値とから生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

(5) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と

前記第1の鍵のもとになる情報と前記特定の認証子値とから生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第1の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送する伝送手段と、
を設けたことを特徴とするコンテンツ情報伝送装置。

(6) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と

前記第1の鍵のもとになる情報と前記特定の認証子値とから生成された第1の

鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第 1 の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、

を設けたことを特徴とするコンテンツ情報記録装置。

(7) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とする伝送媒体。

(8) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報と前記特定の認証子値とから生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とする記録媒体。

(9) 前記ID情報は、1つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別IDに関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーナーリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに関する情報、課金に関する情報のうちの1つ以上の情報であることを特徴とする上記(3)記載のコンテンツ情報伝送方法、または上記(4)記載のコンテンツ情報記録方法、または上記(5)記載のコンテンツ情報伝送装置、または上記(6)記載のコンテンツ情報記録装置、または上記(7)記載の伝送媒体、または上記(8)記載の記録媒体。

(10) 所定の縮退関数により特定の認証子値が得られるように設定されたID

情報を含む第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

(1 1) 所定の縮退関数により特定の認証子値が得られるように設定された ID 情報を含む第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とするコンテンツ情報記録方法。

(1 2) 所定の縮退関数により特定の認証子値が得られるように設定された ID 情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記 ID 情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

(1 3) 所定の縮退関数により特定の認証子値が得られるように設定された ID 情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記 ID 情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とするコンテンツ情報記録方法。

(1 4) 所定の縮退関数により特定の認証子値が得られるように設定された ID 情報を含む第 1 の鍵のもとになる情報に対し、少なくとも前記 ID 情報部分を暗号化して得た暗号化第 1 の鍵のもとになる情報を出力する第 1 の鍵情報暗号化手段と、

前記第 1 の鍵のもとになる情報から生成された第 1 の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と

前記暗号化第 1 の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送す

る伝送手段と、

を設けたことを特徴とするコンテンツ情報伝送装置。

(15) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第1の鍵のもとになる情報を出力する第1の鍵情報暗号化手段と、

前記第1の鍵のもとになる情報から生成された第1の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第1の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、

を設けたことを特徴とするコンテンツ情報記録装置。

(16) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第1の鍵のもとになる情報と、

前記第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とする伝送媒体。

(17) 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第1の鍵のもとになる情報と、

前記第1の鍵のもとになる情報から生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とする記録媒体。

(18) 前記ID情報は、1つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別IDに関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報

、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに関する情報、課金に関する情報のうちの1つ以上の情報であることを特徴とする上記（12）記載のコンテンツ情報伝送方法、または上記（13）記載のコンテンツ情報記録方法、または上記（14）記載のコンテンツ情報伝送装置、または上記（15）記載のコンテンツ情報記録装置、または上記（16）記載の伝送媒体、または上記（17）記載の記録媒体。

【0006】

【発明の実施の形態】

図1に本発明のコンテンツ情報記録装置またはコンテンツ情報伝送装置の第1実施例の概略構成を示す。なお、本説明においては、磁気記録媒体、光記録媒体、半導体メモリ等を記録媒体と呼び、光ケーブル、電線、無線伝送路等の信号を伝送する伝送媒体を伝送路と呼ぶこととする。

【0007】

まず、記録側または送信側（伝送側）の説明をする。図1に示すように、一方向性関数演算装置1は、第1の鍵のもとになる情報から一方向性の関数を用いて原始鍵を作成する。第1の鍵のもとになる情報は、例えば図3に示すように、16ビットのコンテンツプロバイダーIDと、同じく16ビットのコンテンツオーナーIDと、4ビットのメーカーIDと、システム固有の20ビットの情報の計56ビットで構成する。

【0008】

一方向性関数とは、一方向性ハッシュ関数とも表現でき、関数 h とその定義域のある値 x が与えられて $h(x) = h(y)$ となるような y を求めることが困難な関数のことである。コンテンツはMPEGなどの所定の圧縮方式によって圧縮された後、DESなどの暗号化を用いる。DES暗号化方式は1977年にアメリカ連邦政府標準に採用されたもので代表的な共通鍵暗号化方式で56ビットの鍵を用いて64ビット単位で暗号化復号化を行うブロック暗号化方式である。暗号化は64ビットの平分を32ビットづつに分割して転置、置換、非線型関数、排他的論理和により構成されている。例えばDESの場合、暗号化鍵は56ビット程度である。従って

、一方向性関数の出力ビット数が56ビットになるような第1の鍵のもとになる情報は、例えば図3のように全体の長さを56ビットの情報としておく。

【0009】

一方向性関数演算装置1で生成された原始鍵は、コンテンツ鍵生成器2に入力される。また、コンテンツ鍵生成器2には、予め設定された所定の認証子値が、メモリーもしくはCPU等を備えた認証値子発生器3から入力される。

【0010】

なお、所定の認証子値（特定の認証子値）が、後述する再生側の所定の縮退関数により得られるように、縮退関数のパラメータとなる前記ID情報（第1の鍵のもとになる情報に含まれる前記ID情報：図3に示す例ではコンテンツプロバイダーIDと、同じく16ビットのコンテンツオーナーIDと、4ビットのメーカーID）の値を設定しておく。このID情報は正規の使用者にのみ公開されるものであり、許可されたID情報とも呼べるものである。

【0011】

コンテンツ鍵生成器2は、入力された原始鍵の情報と認証子の情報を用いて、所定の関数により第1の鍵（コンテンツ鍵）を生成する。例えば、図4に示すように、原始鍵情報と認証子情報との排他的論理和を計算することで第1の鍵（コンテンツ鍵）を生成する。

【0012】

生成された第1の鍵を用いて、コンテンツ情報をコンテンツ情報暗号化装置4により暗号化する。そして、暗号化コンテンツ情報を記録または伝送する。暗号化にはDESなどの暗号化方式を用いる。

【0013】

記録媒体に記録、もしくは伝送媒体により伝送される情報は、暗号化されたコンテンツ情報（暗号化コンテンツ情報）と、第1の鍵のもとになる情報である。なお、第1の鍵のもとになる情報を、少なくとも前記ID情報部分を暗号化して暗号化された第1の鍵のもとになる情報（暗号化第1の鍵のもとになる情報）として記録または伝送するようにしてもよい。

【0014】

次に、再生側または受信側の説明をする。記録媒体から再生された、もしくは伝送媒体により伝送されてきた第 1 の鍵のもとになる情報から、一方向性関数演算装置 5 により一方向性関数を用いて原始鍵を生成する。暗号化された第 1 の鍵のもとになる情報が供給された場合は、その情報を復号化して第 1 の鍵のもとになる情報を得てから原始鍵を生成する。

【 0 0 1 5 】

また、第 1 の鍵のもとになる情報に含まれている前記 ID 情報を用いて、縮退関数演算装置 6 により前記した認証子値を生成する。縮退関数演算装置 6 に用いる縮退関数は、一方向性関数演算装置 5 に用いる一方向性関数とは別の関数としてもよい。

【 0 0 1 6 】

縮退関数は、例えば図 6 に示すように、ID 情報である 1 6 ビットのコンテンツプロバイダー ID と、同じく 1 6 ビットのコンテンツオーナー ID と、4 ビットのメーカー ID との情報の排他的論理和を求めるような関数でもよい。

【 0 0 1 7 】

一方向性関数演算装置 5 により生成された原始鍵の情報と、縮退関数演算装置 6 により生成された認証子値の情報とは、コンテンツ鍵生成器 7 に入力され、所定の関数により第 1 の鍵（コンテンツ鍵）が生成される。所定の関数は、例えば図 5 に示す原始鍵の情報と、認証子値の情報との 2 つの情報に対して排他的論理和を計算するような関数でよい。

【 0 0 1 8 】

この生成された第 1 の鍵（コンテンツ鍵）を用いて、記録媒体から再生された、もしくは伝送媒体により伝送された暗号化コンテンツ情報をコンテンツ情報復号化装置 8 で復号化する。これによってコンテンツ情報を再生することが可能となる。

【 0 0 1 9 】

前述したように、所定の認証子値（特定の認証子値）が所定の縮退関数により得られるように、第 1 の鍵のもとになる情報に含まれる ID 情報の値が設定されている。この ID 情報は正規の使用者にのみ公開されるものである。従って、不正な

使用者が適当な値のID情報により暗号化コンテンツ情報を復号化しようとしても、特定の認証子値が得られないので復号化できない。また、所定の縮退関数の情報も正規の使用者にのみ公開されるものであるので、たとえID情報の値が漏洩したとしても、その情報から直ちに正規の特定の認証子値がえられものではない。このように上記実施例は、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするものである。

【 0 0 2 0 】

次に、第2実施例について図2と共に説明する。この実施例は、コンテンツ情報の暗号化側において、認証子値を第1の鍵（コンテンツ鍵）生成に反映しないものである。図2において図1と同一の部分には同一の符号を付す。

【 0 0 2 1 】

まず、記録側または送信側（伝送側）の説明をする。図2に示すように、一方向性関数演算装置1は、第1の鍵のもとになる情報から一方向性の関数を用いて原始鍵を作成する。第1の鍵のもとになる情報は、例えば図3に示すように、16ビットのコンテンツプロバイダーIDと、同じく16ビットのコンテンツオーナーIDと、4ビットのメーカーIDと、システム固有の20ビットの情報の計56ビットで構成する。

【 0 0 2 2 】

一方向性関数演算装置1で生成された原始鍵はそのまま第1の鍵（コンテンツ鍵）となり、この第1の鍵を用いて、コンテンツ情報をコンテンツ情報暗号化装置4により暗号化する。そして、暗号化コンテンツ情報を記録または伝送する。暗号化にはDESなどの暗号化方式を用いる。

【 0 0 2 3 】

なお、第1の鍵のもとになる情報に含まれる前記ID情報（コンテンツプロバイダーIDと、同じく16ビットのコンテンツオーナーIDと、4ビットのメーカーID）は、第1実施例と同様に再生側で所定の縮退関数のパラメータとなるものであり、ID情報の値は、予め設定された所定の認証子値（特定の認証子値）が、所定の縮退関数により得られるように設定されたものである。このID情報は、当然正

規の使用者にのみ公開されるものである。

【 0 0 2 4 】

記録媒体に記録もしくは伝送媒体により伝送される情報は、暗号化されたコンテンツ情報（暗号化コンテンツ情報）と、第 1 の鍵のもとになる情報である。なお、第 1 の鍵のもとになる情報を、少なくとも前記 ID 情報部分を暗号化して暗号化された第 1 の鍵のもとになる情報（暗号化第 1 の鍵のもとになる情報）として記録または伝送するようにしてもよい。

【 0 0 2 5 】

次に、再生側または受信側の説明をする。記録媒体から再生された、もしくは伝送媒体により伝送されてきた第 1 の鍵のもとになる情報から、一方向性関数演算装置 5 により一方向性関数を用いて原始鍵を生成する。この原始鍵がそのまま第 1 の鍵（コンテンツ鍵）となる。暗号化された第 1 の鍵のもとになる情報が供給された場合は、その情報を復号化して第 1 の鍵のもとになる情報を得てから原始鍵を生成する。

【 0 0 2 6 】

また、第 1 の鍵のもとになる情報に含まれている前記 ID 情報を用いて、縮退関数演算装置 6 により前記した認証子値を生成する。縮退関数演算装置 6 に用いる縮退関数は、一方向性関数演算装置 5 に用いる一方向性関数とは別の関数としてもよい。

【 0 0 2 7 】

縮退関数は、例えば図 6 に示すように、16 ビットのコンテンツプロバイダー ID と、同じく 16 ビットのコンテンツオーサー ID と、4 ビットのメーカー ID との情報の排他的論理和を求めるような関数でもよい。

【 0 0 2 8 】

一方向性関数演算装置 5 により生成された原始鍵、即ち第 1 の鍵（コンテンツ鍵）の情報と、縮退関数演算装置 6 により生成された認証子値の情報とは、コンテンツ鍵加工器 11 に入力される。コンテンツ鍵加工器 11 は前記予め設定されている特定の認証値子の情報が供給された場合のみ、入力される第 1 の鍵（コンテンツ鍵）の情報をそのまま出力するものであり、特定の認証値子以外の情報が

供給された場合には、入力される第 1 の鍵情報を加工して（値を変更して）出力する。

【 0 0 2 9 】

コンテンツ鍵加工器 1 1 から出力された第 1 の鍵（コンテンツ鍵）を用いて、記録媒体から再生された、もしくは伝送媒体により伝送された暗号化コンテンツ情報をコンテンツ情報復号化装置 8 で復号化する。正規の特定の認証値子がコンテンツ鍵加工器 1 1 に供給されれば、正しい第 1 の鍵（コンテンツ鍵）がコンテンツ情報復号化装置 8 に入力され、これによってコンテンツ情報を再生することが可能となる。

【 0 0 3 0 】

このように本実施例によれば、正規の特定の認証値子が得られないければ暗号化コンテンツ情報を復号化できず、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするものである。

【 0 0 3 1 】

次に、第 3 実施例について図 7 と共に説明する。本実施例において、コンテンツ情報の暗号化側（記録側または送信側）は図 2 に示す第 2 実施例と同様であるので、ここでは、再生側または受信側について説明する。

【 0 0 3 2 】

記録媒体から再生された、もしくは伝送媒体により伝送されてきた第 1 の鍵のもとになる情報から、一方向性関数演算装置 5 により一方向性関数を用いて原始鍵を生成する。この原始鍵がそのまま第 1 の鍵（コンテンツ鍵）となる。暗号化された第 1 の鍵のもとになる情報が供給された場合は、その情報を復号化して第 1 の鍵のもとになる情報を得てから原始鍵を生成する。

【 0 0 3 3 】

また、第 1 の鍵のもとになる情報に含まれている前記 ID 情報を用いて、縮退関数演算装置 6 によって認証子値を生成する。縮退関数演算装置 6 に用いる縮退関数は、一方向性関数演算装置 5 に用いる一方向性関数とは別の関数としてもよい。

【 0 0 3 4 】

縮退関数は、例えば図 6 に示すように、16 ビットのコンテンツプロバイダー ID と、同じく 16 ビットのコンテンツオーナー ID と、4 ビットのメーカー ID との情報の排他的論理和を求めるような関数でもよい。

【 0 0 3 5 】

縮退関数演算装置 6 により生成された認証子値は、認証子値正当性判定器 12 に供給され、正規の特定の認証値子であるか否かが判定される。認証子値正当性判定器 12 の判定結果はコンテンツ情報復号化装置 8 a に供給され、コンテンツ情報復号化装置 8 a は、判定結果が「正規の特定の認証値子」である場合のみ復号動作を行う。

【 0 0 3 6 】

上記判定結果が「正規の特定の認証値子」である場合には、コンテンツ情報復号化装置 8 a は、一方向性関数演算装置 5 により生成された第 1 の鍵（コンテンツ鍵）を用いて、記録媒体から再生された、もしくは伝送媒体により伝送された暗号化コンテンツ情報を復号化する。これによってコンテンツ情報を再生することが可能となる。

【 0 0 3 7 】

このように本実施例によれば、正規の特定の認証値子を得られないければ暗号化コンテンツ情報を復号化できず、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするものである。

【 0 0 3 8 】

なお、第 1 の鍵のもとになる情報に含まれる前記 ID 情報としては、1 つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別 ID に関する情報、複数人のグループを識別する識別 ID に関する情報、レーティングに関する情報、機器メーカーの識別 ID に関する情報、コンテンツプロバイダーの識別 ID に関する情報、時間に関する情報、コンテンツオーナーリング者に関する情報、コンテンツを再生する再生機器の固有 ID に関する情報、接続機器の固有 ID に関する情報、コンテンツの記録されたメディアの固有 ID に関する情報、コンテンツを識別する ID に

関する情報、課金に関する情報のうちの1つ以上の情報を用いることが考えられる。

【 0 0 3 9 】

【発明の効果】

以上の通り、本発明によれば、正規のID情報にもとづく正規の特定の認証値子
が得られないければ暗号化コンテンツ情報を復号化できないので、不正な条件下
でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生
（復号）を的確に行うことを可能とする。

【図面の簡単な説明】

【図 1】

第 1 実施例の概略構成を示す図である。

【図 2】

第 2 実施例の概略構成を示す図である。

【図 3】

第 1 の鍵のもとになる情報の構成例を示す図である。

【図 4】

図 1 に示す暗号化側のコンテンツ鍵生成器の説明図である。

【図 5】

図 1 に示す復号化側のコンテンツ鍵生成器の説明図である。

【図 6】

復号化側の縮退関数の例を示す図である。

【図 7】

第 3 実施例の概略構成を示す図である。

【符号の説明】

- 1, 5 一方向性関数演算装置
- 2, 7 コンテンツ鍵生成器
- 3 認証子値発生器
- 4 暗号化装置
- 6 縮退関数演算装置

8 コンテンツ情報復号化装置

【書類名】 図面

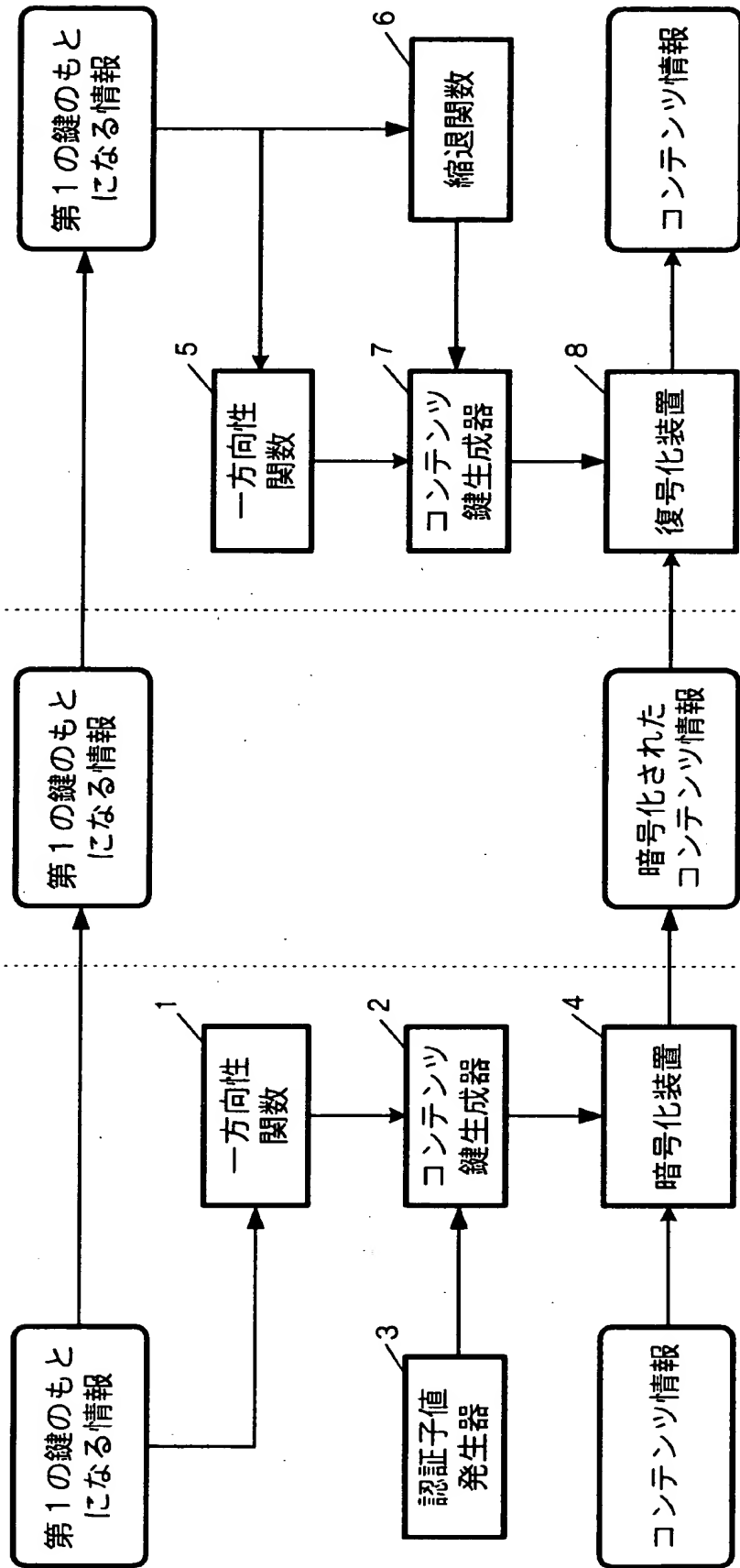
【図 1】

再生側または受信側

記録媒体または伝送路

記録側または送信側

図 1



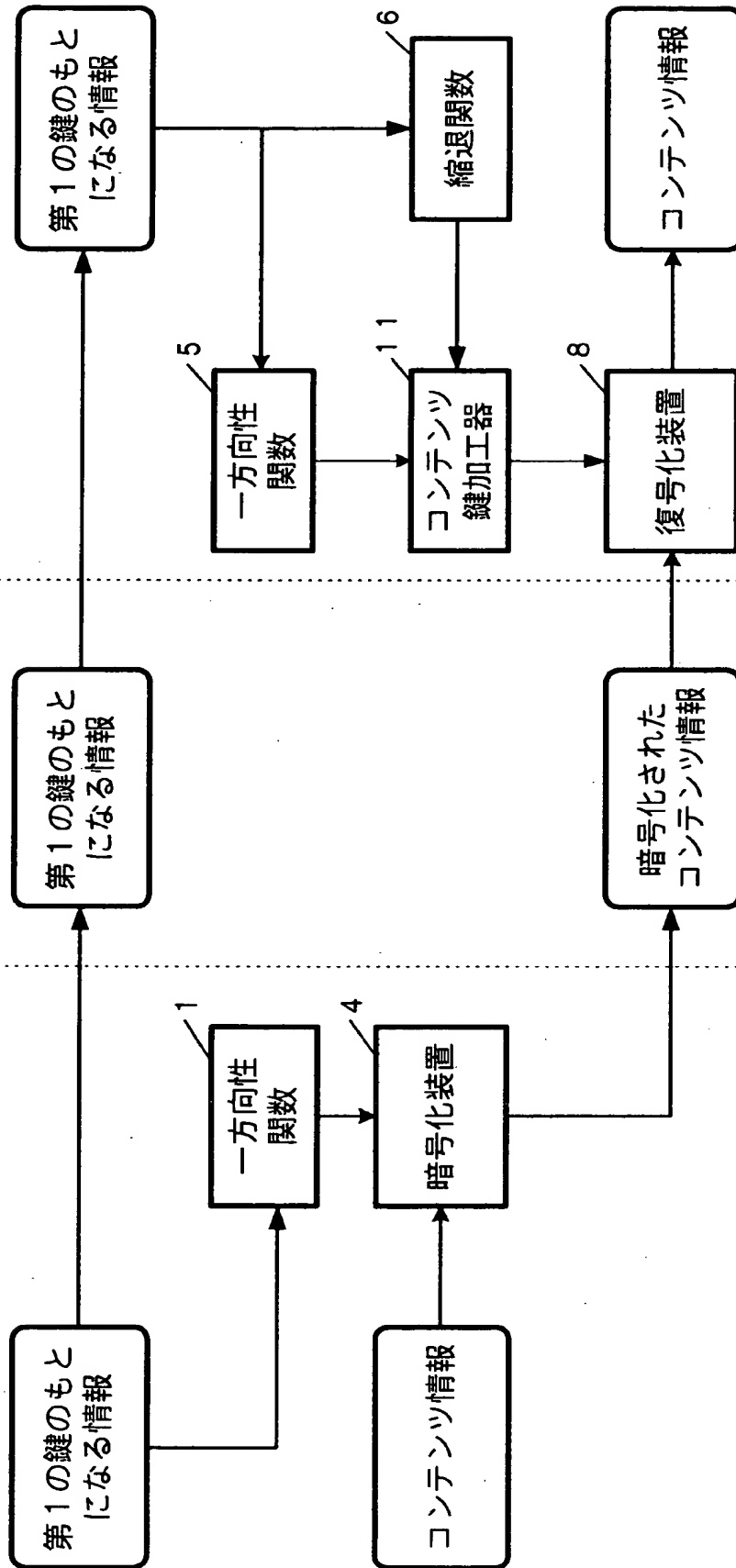
【図 2】

再生側または受信側

記録媒体または伝送路

記録側または送信側

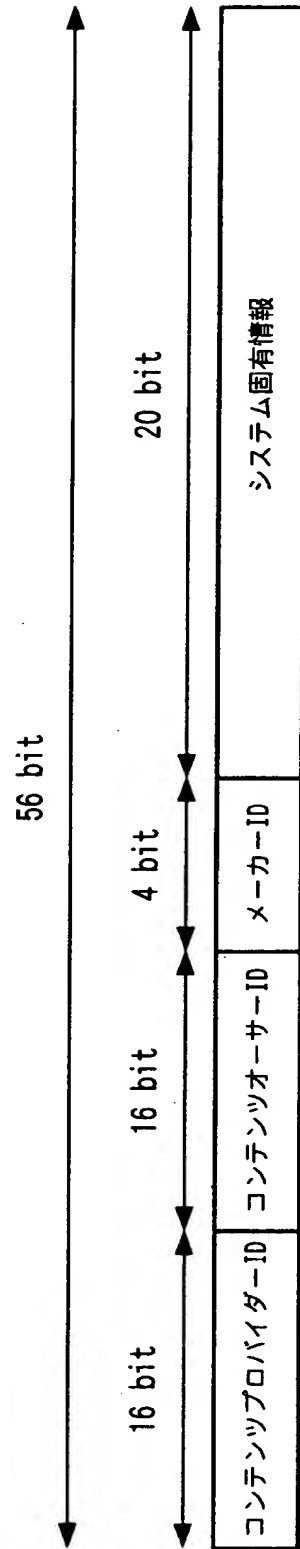
図 2



【図 3】

第 1 の 鍵 の も と に な る 情 報

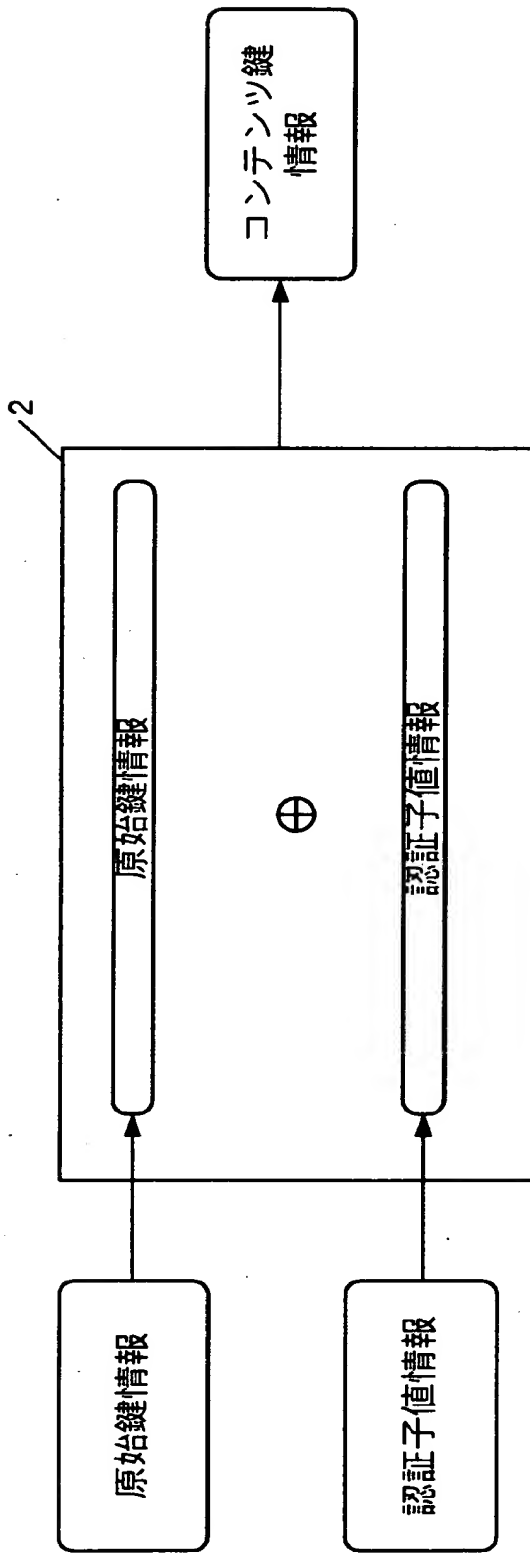
図 3



特 2 0 0 0 - 0 1 8 4 3 7

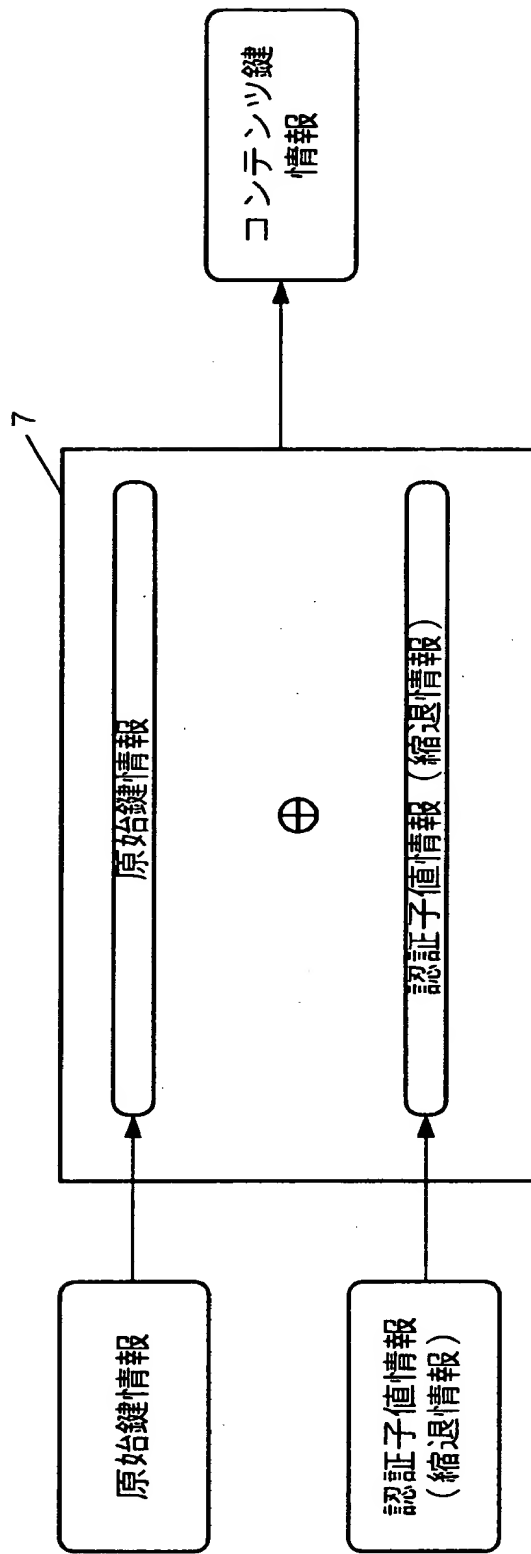
【図 4】

図 4



【図 5】

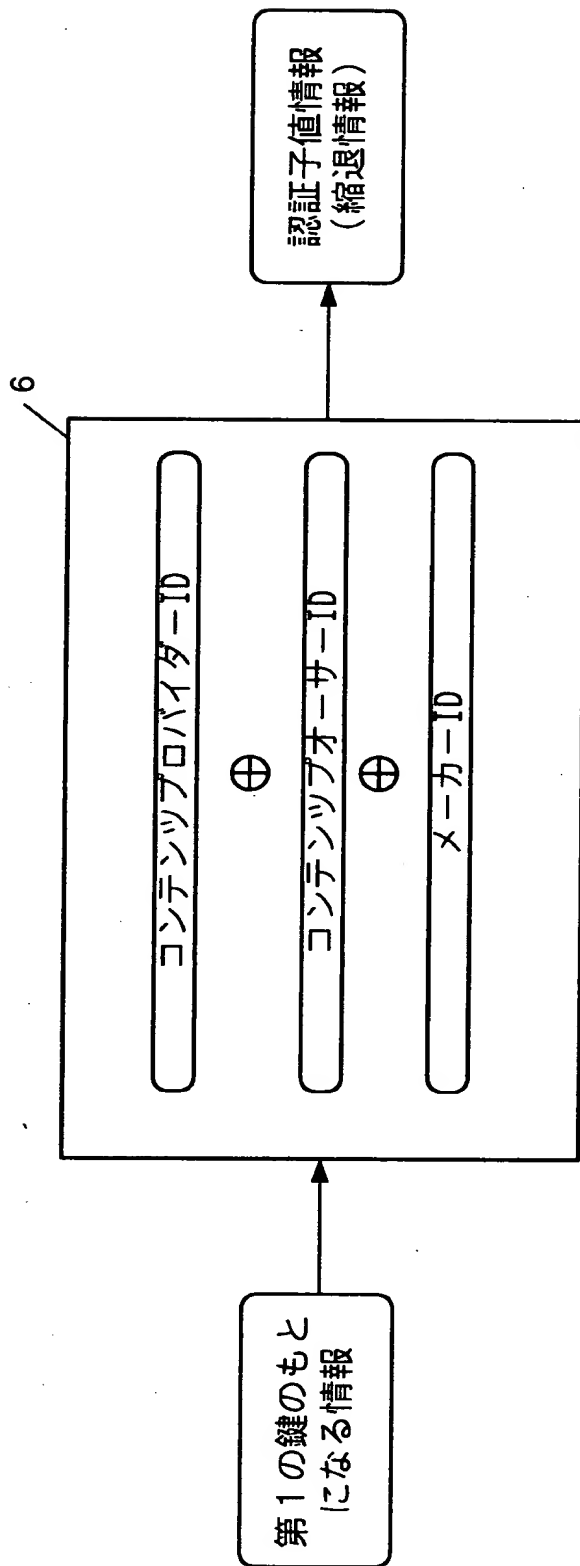
図 5



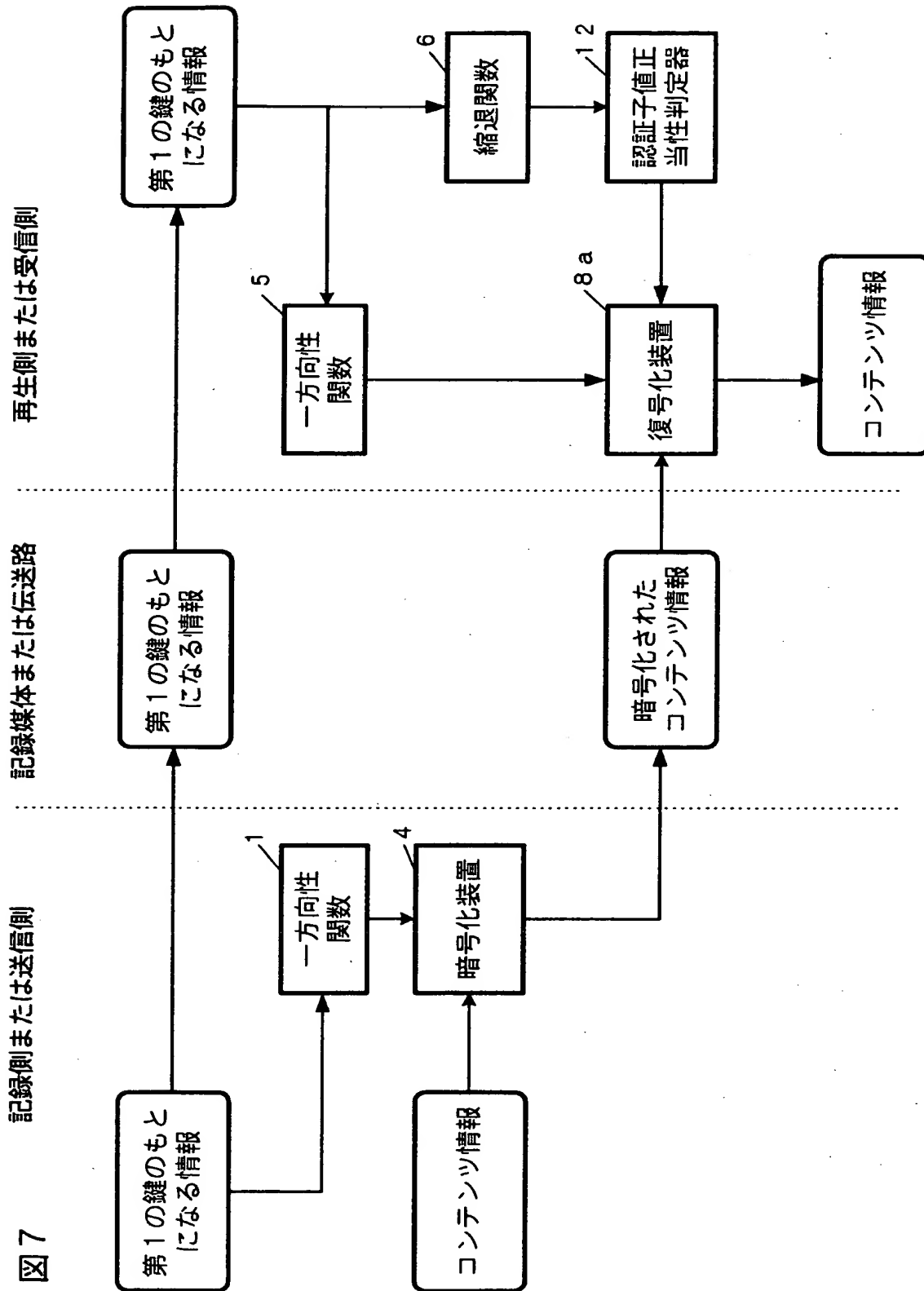
特 2 0 0 0 - 0 1 8 4 3 7

【図 6】

図 6



【図 7】



【書類名】 要約書

【要約】

【課題】 暗号化コンテンツ情報を正規の制限下においてのみの確に再生（復号）させることを可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供すること。

【解決手段】 所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第1の鍵のもとになる情報と、前記第1の鍵のもとになる情報と前記特定の認証子値とから生成された第1の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報とを伝送または記録する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日	1990年 8月 8日
[変更理由]	新規登録
住 所	神奈川県横浜市神奈川区守屋町3丁目12番地
氏 名	日本ビクター株式会社